



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

HN

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/881,899	06/14/2001	Chee-Hong Wong	23615-05503	8876
21919	7590	12/30/2005	EXAMINER	
MEREK, BLACKMON & VOORHEES, LLC 673 S. WASHINGTON ST. ALEXANDRIA, VA 22314			SON, LINH L D	
		ART UNIT	PAPER NUMBER	
		2135		
DATE MAILED: 12/30/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/881,899	WONG ET AL.	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 14 June 2001.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-26 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date <u>09/26/2005</u> .	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

1. This Office Action is responding to the Amendment received on 09/26/2005.
2. Claims 1-26 are pending.

Response to Arguments

3. Applicant's arguments, see Amendment, filed 09/26/2005, with respect to the rejection(s) of claim(s) 1-26 under ***35 USC § 103(a)*** have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Dorenbos and Smith. See below.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2135

5. Claims 1-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dorenbos, US Patent No. 5751813, in view of Smith et al, US Patent No. 6061448, hereinafter "Smith".

6. As per claim 1:

Dorenbos teaches "A computer-implemented method for securely transmitting an information package from a sender to an addressee via a network (Fig. 1), the method comprising a server system performing the steps of: receiving a delivery from the sender, the delivery comprising: the information package encrypted with a package encryption key (Fig 2, User Private key); and a package decryption key (User ID) encrypted with an escrow key (Fig 2, #105, Encryption Server Public key); storing the delivery in escrow for the addressee; sending to the addressee a notification of the delivery; and in response to receiving an acknowledgement from the addressee: obtaining a new public key of the addressee (Fig 4 # 409, Col 4 lines 55-60); decrypting the package decryption key (Col 3 lines 26-30); encrypting the package decryption key with the addressee's new public key (Col 3 lines 32-36, and Col 4 lines 55-60); and transmitting to the addressee the information package encrypted with the package encryption key and the package decryption key encrypted with the addressee's new public key (Col 3 lines 32-38).

However, Dorenbos does not directly teach of the decryption key.

Nevertheless, Dorenbos teaches of encrypting the User ID of the sender with the package and the receiver or addressee uses the User ID to obtain the correct decryption key to decrypt the message. Therefore, it would have been obvious at the

time of the invention was made for one ordinary skill in the art to modify Dorenbos invention to include the encryption key with the delivery so that the user does not need to store the sender key to decrypt the message.

Further, Dorenbos does not teach of storing the delivery in escrow for the addressee; sending to the addressee a notification of the delivery; and in response to receiving an acknowledgement from the addressee:

Nevertheless, Smith discloses a "Method and System for Dynamic Server Document Encryption" invention, which including a server computer sends, receives, and stores secure data provided by authorized users. Server computer receives the encrypted document from user, stores it securely, and sends notification to the recipient. In response to the recipient response, the server sends the delivery to the recipient (Col 5 lines 5-30).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Dorenbos's invention to incorporate Smith's storage and notification feature to make sure that the user is ready to receive the delivery.

7. As per claims 11, and 18:

Dorenbos teaches "A system, a method and an apparatus for securely transmitting an information package from a sender to an addressee via a network (Fig. 1), the system comprising: a storage module, comprising a computer-readable storage medium, for receiving, and storing in escrow, a delivery from the sender, said delivery comprising: a package decryption key (User ID) encrypted with an escrow key, and the information

package encrypted with a package encryption key (Fig 2, #105, Encryption Server Public key); a notification module coupled to the storage module, for sending a notification to the addressee via the network; a key registration module coupled to the notification module for, in response to receiving an acknowledgement from the addressee, receiving a new public key of the addressee; and a transmission module coupled to the storage module, for decrypting the package decryption key and re-encrypting the package decryption key with the new public key of the addressee (Col 3 lines 32-36, and Col 4 lines 55-60), and for transmitting to the addressee the information package encrypted with the package encryption key and the package decryption key encrypted with the addressee's new public key (Col 3 lines 32-38).

However, Dorenbos does not directly teach of the decryption key.

Nevertheless, Dorenbos teaches of encrypting the User ID of the sender with the delivery and the receiver or addressee uses the User ID to obtain the correct decryption key to decrypt the message. Therefore, it would have been obvious at the time of the invention was made for one ordinary skill in the art to modify Dorenbos invention to include the encryption key with the delivery so that the user does not need to store the sender key to decrypt the message.

Further, Dorenbos does not teach of a notification module coupled to the storage module, for sending a notification to the addressee via the network; a key registration module coupled to the notification module for, in response to receiving an acknowledgement from the addressee, receiving a new public key of the addressee.

Nevertheless, Smith discloses a "Method and System for Dynamic Server Document Encryption" invention, which including a server computer sends, receives, and stores secure data provided by authorized users. Server computer receives the encrypted document from user, stores it securely, and sends notification to the recipient. In response to the recipient response, the server sends the delivery to the recipient (Col 5 lines 5-30). Further, Smith also teaches of a key registration module to receive a new public key of the recipient or addressee (Col 5 lines 9-19).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Dorenbos's invention to incorporate Smith's storage and notification feature to make sure that the user is ready to receive the delivery.

8. As per claims 2 and 19:

Dorenbos and Smith teach "The method of claims 1 and 18". Further Smith discloses "the server system performing the steps of: receiving a request from the sender for a public key of the addressee; determining whether the addressee has a public key; and in response to not finding a public key of the addressee: transmitting the escrow key to the sender" in (Col 5 lines 5-15).

9. As per claims 3 and 20:

Dorenbos and Smith teach "The method of claims 2 and 19". Wherein Smith discloses "the step of determining whether the addressee has a public key comprises the

Art Unit: 2135

sub-step of: checking a public key database for a public key of the addressee" in (Col 6 lines 40-65).

10. As per claims 4 and 21:

Dorenbos and Smith teach "The method of claims 1 and 18". Further Smith discloses "the server system performing the steps of: in response to the sender searching a public key database for a public key of the addressee and not finding a public key of the addressee: receiving a request from the sender for the escrow key; and transmitting the escrow key to the sender" in (Col 6 lines 40-65).

11. As per claims 5, 13-14, and 22:

Dorenbos and Smith teach "The method of claims 1, 11, and 18". Further Smith discloses "the server system performing the steps of: registering and issuing the new public key to the addressee; and storing the addressee's new public key in a public key database" in (Col 5 lines 1-15).

12. As per claims 6 and 15:

Dorenbos and Smith teach "The method of claims 1 and 11". Wherein Smith discloses "the escrow key is one of a group comprising a symmetric key and an asymmetric key" in (Col 4 lines 8, asymmetric key equals to public/private key).

13. As per claims 7, 16, and 23:

Dorenbos and Smith teach "The method of claims 1, 11, and 18". Wherein Smith discloses "the notification is one of a group comprising an e-mail notification, a desktop

Art Unit: 2135

notification, a voice notification, a pager notification, and a facsimile notification" in (Col 5 lines 1-15).

14. As per claims 8 and 24:

Dorenbos and Smith teach "The method of claims 1 and 18". Further Smith discloses "the server system performing the steps of: receiving from the sender a digest of one from a group comprising: the information package; the information package encrypted with the package encryption key; and the information package encrypted with the package encryption key and the package decryption key encrypted with the escrow key; and in response to receiving the acknowledgement from the addressee: transmitting the digest to the addressee" in (Col 5 lines 1-30, and Col 6 lines 40-67).

15. As per claims 9, 25:

Dorenbos and Smith teach "The method of claims 8 and 25". Wherein Smith discloses "the digest is encrypted by a private key of the sender" in (Col 3 lines 1-6).

16. As per claim 12:

Dorenbos and Smith teach "The system of claim 11". Further Smith discloses "a directory interface coupled to the storage module for checking, in response to receiving a request from the sender for a public key of the addressee, a public key database for the public key of the addressee; and an escrow key manager coupled to the directory interface for providing, in response to the directory interface failing to obtain a public key of the addressee from the public key database, an escrow key for encrypting the

package decryption key" in (Col 5 lines 1-52, public key of the addressee is interpreted as the escrow key).

17. As per claims 10, 17, and 26:

Dorenbos and Smith teach "The computer-readable medium of claims 1, 11, and 18". Further Smith discloses "program code adapted to perform the step of: authenticating the addressee prior to transmitting the information package encrypted with the package encryption key and the package encryption key encrypted with the addressee's new public key" in (Col 5 lines 1-53) and the rejection of claim is incorporated.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135


